# NIAC Working Group on Prioritization of Cyber Vulnerabilities

## Working Group Update

Martin G. McGuinn, Chairman & CEO
Mellon Financial Corporation

Tuesday – April 13, 2004

# Presentation Outline

- Background
- Report on Actions to Date
- Survey Content
- Next Steps
- Appendix

# Background

- October 14 – NIAC Members recommend establishing a working group to answer the question – "Are we ranking areas vulnerable to a cyber attack?"

# Deliverables

- Summary of the types of Cyber Attacks
- Analysis of which Critical Infrastructures are vulnerable to those attacks – and rank if appropriate
- Summary of mitigants/protective measures
- Summary of implications/ramifications associated with successful attacks (based on results of a "Vulnerability Assessment Survey" customized for each critical infrastructure)

# Report on Actions Taken to Date

- BGP Security Research Summary — Jan. 28
  - Cisco Systems
- Draft survey developed and vetted — Feb. 2
- Cyber Attack Economics Report — Feb. 25
  - Scott Borg, Senior Research Fellow *
- Health Care sector sample — Mar. 9
- Survey revised to reflect Borg model — Mar. 15

* *Institute for Security Technology Studies, Dartmouth College*

# Cyber-Attack Models

**Types of Cyber Incidents (CERT)**

- Probe
- Scan
- Account Compromise
- Root Compromise
- Packet Sniffer
- Denial of Service
- Exploitation of Code
- Internet Infrastructure Attacks

**Information Security Model**

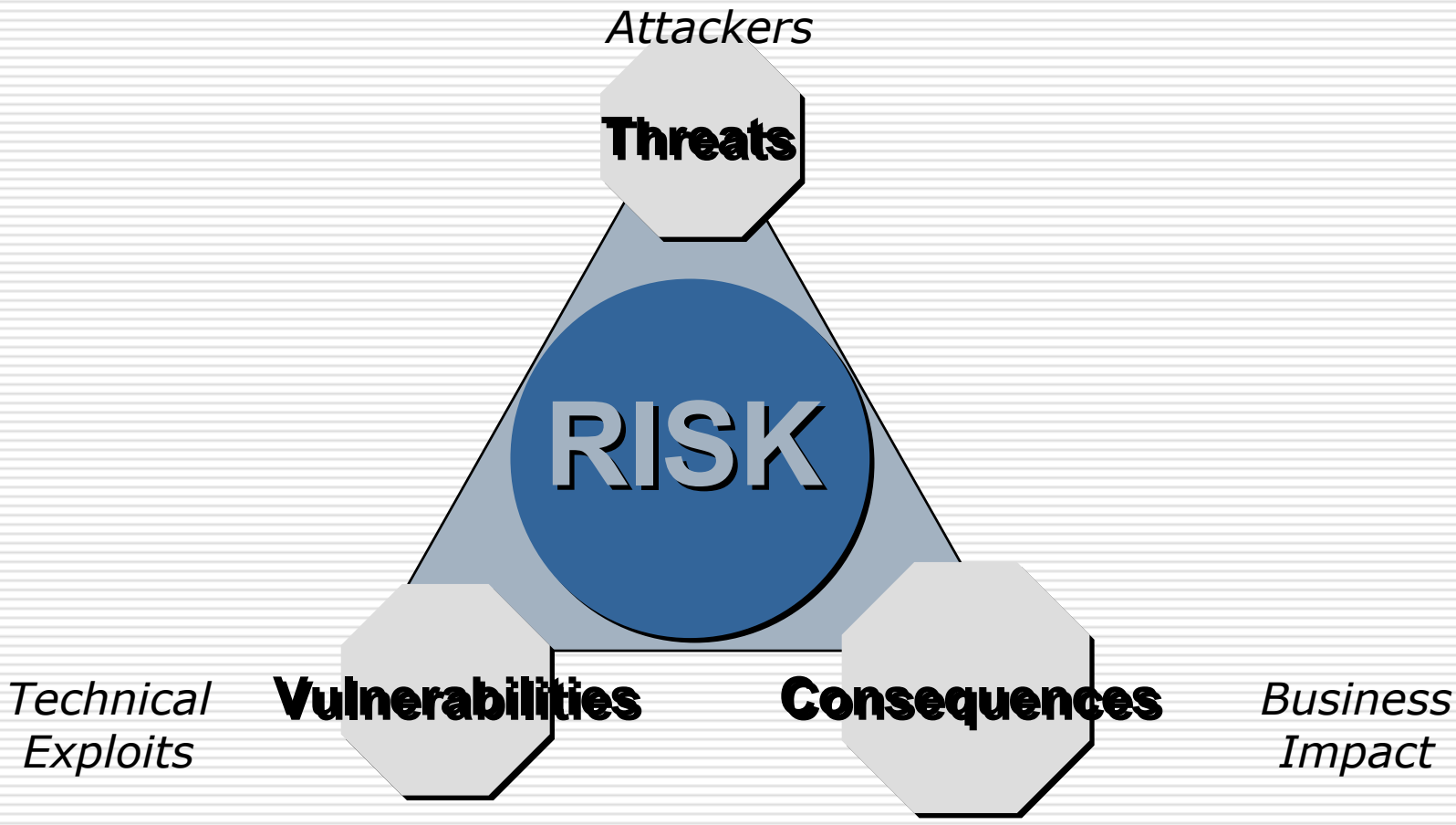
- Confidentiality
- Availability
- Integrity
- Authentication
- Non-repudiation

**Business Categories (Borg Model)**

- Interruption of data in order to interrupt business operations
- Corruption of data in order to cause it to operate defectively
- Obfuscation of data, causing people to be in the wrong business
- Publication of confidential data, undermining the ability to engage in any business

*Technical Exploit* → *Compromises Security* → *Business Impact*

# Risk = Threats x Vulnerabilities x Consequences



# Survey Content

- Identification of key information systems and what they accomplish
- Economic metrics of these systems
- Implications to National Security/Emergency Preparedness
- Dependency on any other network based critical infrastructure
- Dependency of a critical infrastructure on this service

# Survey Content

- Evaluate the possible consequences of "types" of cyber attacks on each of the identified key systems:
  - Interruption of business operations
  - Business operates in a defective way
  - Distrust of the system
  - Undermine the ability to engage in that business

# Survey Content

- Identifying what alternatives might be utilized in the event of a sustained attack on each of these systems

# Next Steps

| | |
|---|---|
| Finalize survey | April 14 |
| Survey distribution | April 21 |
| Survey returned | May 26 |
| Compilation and analysis | June 30 |
| Deliverable | July 13 |

# Appendix

- Working Group Participants

# Study Group Participants

- Susan Vismor, Mellon Financial Corp., Study Group Chair
- Teresa C. Lindsey, BITS
- Peter Allor – Internet Security Systems
- Bruce Larsen – American Water
- Chris Terzich - Wells Fargo & Company
- Ken Watson - Cisco Systems, Inc.
- Dan Bart, TIA
- David Thompson, TIA
- Lou Leffler, North American Electric Power
- Tim Zoph, Northwestern Memorial Hospital
- Scott Borg, Institute for Security Technology Studies, Dartmouth College
- Nancy Wong, DHS
- David Sanders, DHS, National Cyber Security Division